Claims

1. A postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type requiring electrical power to maintain the contents thereof, said postal security device also comprising a battery powering the second memory and a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory is disconnected from the battery, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine, said body of data encrypted by the cryptographic engine with respect to the encryption key.

2. A method for use with a postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type that requires electric power to maintain its contents, said postal security device also comprising a battery powering the second memory and a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory is disconnected from the battery, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine; the method comprising the steps of:

storing the encryption key within the second memory;

encrypting the body of data by the cryptographic engine with respect to the encryption key;

storing the encrypted body of data in the first memory; and

in the event of tampering, removing power from the second memory.

3. A method for use with a postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type that clears its contents upon a predetermined electrical condition, said postal security device also comprising a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory has said predetermined electrical condition, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine; the method comprising the steps of:

storing the encryption key within the second memory;

encrypting the body of data by the cryptographic engine with respect to the encryption key;

storing the encrypted body of data in the first memory; and

in the event of tampering, causing said predetermined electrical condition.